

A2

Best Available Copy

1/5/1 (Item 1 from file: 351)
 DIALOG(R)File 351:Derwent WPI
 (c) 2001 Derwent Info Ltd. All rts. reserv.

012182604 **Image available**
 WPI Acc No: 1998-599517/199851
 XRPX Acc No: N98-466907

Software security system in network - is incorporated into intelligent software module either as encryption, secret key or electronic signature

Patent Assignee: HITACHI LTD (HITA)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 10269186	A	19981009	JP 9771311	A	19970325	199851 B

Priority Applications (No Type Date): JP 9771311 A 19970325

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 10269186	A	6	G06F-015/16	

Abstract (Basic): JP 10269186 A

The security system is incorporated into an intelligent agent which is the software module itself, either by encryption, secret key or electronic signature.

ADVANTAGE - Prevents access to software key unauthorised users of software in network.

Dwg.1/6

Title Terms: SOFTWARE; SECURE; SYSTEM; NETWORK; INCORPORATE; INTELLIGENCE; SOFTWARE; MODULE; ENCRYPTION; SECRET; KEY; ELECTRONIC; SIGNATURE

Derwent Class: T01

International Patent Class (Main): G06F-015/16

International Patent Class (Additional): G06F-009/06; G06F-013/00

File Segment: EPI

1/5/2 (Item 1 from file: 347)
 DIALOG(R)File 347:JAPIO
 (c) 2000 JPO & JAPIO. All rts. reserv.

05986086 **Image available**
 SECURITY PROTECTION SYSTEM FOR AGENT

PUB. NO.: 10-269186 A]
 PUBLISHED: October 09, 1998 (19981009)
 INVENTOR(s): IMAI KOUSUKE
 APPLICANT(s): HITACHI LTD [000510] (A Japanese Company or Corporation), JP (Japan)
 APPL. NO.: 09-071311 [JP 9771311]
 FILED: March 25, 1997 (19970325)
 INTL CLASS: [6] G06F-015/16; G06F-009/06; G06F-013/00; G06F-013/00
 JAPIO CLASS: 45.4 (INFORMATION PROCESSING -- Computer Applications); 45.1 (INFORMATION PROCESSING -- Arithmetic Sequence Units); 45.2 (INFORMATION PROCESSING -- Memory Units)

ABSTRACT

PROBLEM TO BE SOLVED: To prevent a third party from leaking secrecy or illegally using an intelligent agent by allowing the intelligent agent itself to have a security module and protect itself.

SOLUTION: A client machine selects and adds a necessary security mechanism 2 for the agent 1. The selected security mechanism 2 performs a necessary security process to obtain security information 3. The agent 1 moves to a server machine together with the data 4, a security mechanism 2, and security information that it has. The agent 1 after moving onto the server machine performs a security process with a service providing program 10, which provides service on the server machine. Consequently, both the client and server can protect the security without being aware of the security mechanisms that support the opposite sides.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-269186

(43) 公開日 平成10年(1998)10月9日

(51) Int.Cl.⁸G 0 6 F 15/16
9/06
13/00

識別記号

3 7 0
5 5 0
3 5 1
3 5 7

F I

G 0 6 F 15/16
9/06
13/003 7 0 Z
5 5 0 Z
3 5 1 Z
3 5 7 Z

審査請求 未請求 請求項の数 1 O L (全 6 頁)

(21) 出願番号

特願平9-71311

(22) 出願日

平成9年(1997)3月25日

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 今井 厚祐

神奈川県横浜市戸塚区戸塚町5030番地株式

会社日立製作所ソフトウェア開発本部内

(74) 代理人 弁理士 小川 勝男

(54) 【発明の名称】 エージェントのセキュリティ保護方式

(57) 【要約】

【課題】 ネットワーク上のインテリジェントエージェントにおいて、エージェント自身のセキュリティを保護する必要がある。

【解決手段】 エージェント自身にセキュリティモジュールとセキュリティ情報を持たせ、自分自身を保護する能力を持たせる。エージェントのセキュリティ保護を向上させ、またサーバでの不正なエージェントの実行防止などの効果を持つ。

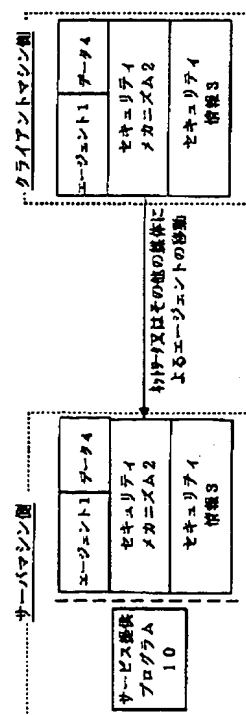


図1

【特許請求の範囲】

【請求項1】 ネットワークを介して自己の判断で移動・実行するインテリジェントエージェントにおいて、エージェント自身がセキュリティモジュールを持ち、自分自身を保護することを特徴とするエージェントのセキュリティ管理方式。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】 エージェントのセキュリティ保護方式に関する。

【0002】

【従来の技術】 エージェントは、自律性、移動性、知性を持つソフトウェアモジュールで、ユーザの依頼を受けると自分自身の判断でネットワーク上を移動し、アプリケーションを自動的に起動し、処理していく。現在、広く研究開発されているエージェント技術ではセキュリティ保護方式について考慮されていなかった。

【0003】 なお、本発明の出願前に知られている最も近い例としては、特公平8-27726公報に記載されているエージェント・コンピュータ管理システムや特開平7-87116公報に記載されているネットワークを管理する方法及び装置が提案されている。しかし、エージェント自身がセキュリティ機能を持つことについてはカバーされていない。

【0004】

【発明が解決しようとする課題】 従来のエージェント技術では、エージェント自身の持つデータの機密性保護、データへのアクセス制御、エージェントとデータの完全性保護、第三者によるエージェントモジュールの不正使用、エージェント起動者の識別、悪意を持つエージェントの実行の強制終了、複数セキュリティメカニズム・アルゴリズムサポートなどについて考慮されていなかったため、不特定多数と接続されている公衆回線などを介して移動、実行するエージェントのセキュリティ保護の問題があった。

【0005】 そこで本発明では、エージェント自身にセキュリティ機能を持たせることにより、エージェントのセキュリティ保護を高めることを考えた。

【0006】 本発明の目的は、エージェントの持つデータの機密性保護を提供することにある。

【0007】 本発明の他の目的は、エージェントの持つデータやエージェント自身へのアクセス制御機能を提供することにある。

【0008】 本発明の他の目的は、エージェントとデータの完全性保護を提供することにある。

【0009】 本発明の他の目的は、第三者によるエージェントモジュールの不正使用の防止機能を提供することにある。

【0010】 本発明の他の目的は、エージェント起動者を識別する機能を提供することにある。

【0011】 本発明の他の目的は、悪意を持つエージェントの実行を強制終了させる機能を提供することにある。

【0012】 本発明の他の目的は、複数セキュリティメカニズム・アルゴリズムをサポートする機能を提供することにある。

【0013】

【課題を解決するための手段】 本発明は、インテリジェントエージェント自身がセキュリティモジュールを持ち、自分自身を保護する手段が提供される。

【0014】

【発明の実施の形態】 図1は本発明の一実施例に基づくエージェントセキュリティを示す図である。本システムは、エージェント1、セキュリティメカニズム2、セキュリティ情報3、サービス提供プログラム10からなる。

【0015】 クライアントマシンでは、エージェント1に対して必要なセキュリティメカニズム2を選択しエージェント1に追加する。セキュリティメカニズム2の選択方法として、サービス提供者に関係なくエージェント起動側のデフォルトのメカニズムを選択する、エージェント起動側に事前に登録されている、サービス提供者がサポートするメカニズムを選択する、エージェント1を起動する前に、サーバマシン側、クライアントマシン側の間でサポートしているセキュリティメカニズムに関して折衝し、選択する、各マシン又はプログラムは、ディレクトリサーバなどの第三者サーバに対してサポートしているセキュリティメカニズムを事前に登録し、クライアントマシン側はその第三者サーバに必要なセキュリティメカニズムを問い合わせることによって選択する。選択されたセキュリティメカニズム2は、必要なセキュリティ処理を行い、セキュリティ情報3を得る。エージェント1は、エージェント1が持つデータ4、セキュリティメカニズム2、セキュリティ情報3と共にサーバマシンへ移動する。エージェント1は、サーバマシン上に移動した後、サーバマシン上でサービスを提供するサービス提供プログラム10との間でセキュリティ処理を行う。

【0016】 図1では、実施例としてクライアントマシン上でセキュリティメカニズム2を追加しているが、エージェント1にセキュリティメカニズム2を追加するためのサーバを使用することも可能である。

【0017】 セキュリティ処理が正常に終了した場合、エージェント1はサービス提供プログラム10からサービスを受ける。

【0018】 次に図2を用いて本発明のセキュリティメカニズム2、セキュリティ情報3の具体的な構成とクライアントマシンでのセキュリティ処理方を説明する。図2に示すように、図1のセキュリティメカニズム2は、ハッシュメカニズム21、暗号・復号メカニズム2

3

2、鍵管理メカニズム23、アクセス制御メカニズム24から構成され、図1のセキュリティ情報3は、ハッシュ値31、エージェント起動者の電子署名32、電子鍵33、アクセス制御情報34から構成される。また、クライアントでは、事前に暗号・復号メカニズム22の処理に必要な、起動者の秘密鍵333、サービス提供者の公開鍵332を保持しておく必要がある。

【0019】ハッシュメカニズム21は任意のデータに対してハッシュ計算を行い、ハッシュ値31を算出する機能を持つモジュールである。

【0020】暗号・復号メカニズム22は任意のデータに対して暗号処理や電子署名32の生成処理、または既に暗号処理されているデータに対して復号処理を行う機能を持つモジュールである。

【0021】鍵管理メカニズム23は暗号・復号・電子署名32の生成処理に必要な電子鍵33の生成、管理機能を持つモジュールである。

【0022】アクセス制御メカニズム24は、エージェント1自身やエージェント1が持つデータ4に対するアクセスを制御するために、アクセスを要求してくる要求者の身元とその要求者の持つアクセス制御情報34から、アクセスを制御する機能を持つモジュールである。アクセス制御情報34は、エージェント生成者又はエージェント起動者によってアクセス制御メカニズム24に提供される。

【0023】クライアントマシンでのセキュリティ処理方式について説明する。クライアントマシンのエージェント起動者は、先に記したセキュリティメカニズムや暗号アルゴリズムから必要なものを選択する。例として、図3を用いて全てのセキュリティメカニズムを選択した場合について説明する。

【0024】まず初めに、ハッシュメカニズム21は保護の対象となるデータのハッシュ値31を算出する。この時に保護の対象となるデータは、エージェント1とデータ4であるが、必要に応じてハッシュメカニズム21、暗号・復号メカニズム22、鍵管理メカニズム23、アクセス制御メカニズム24、エージェント起動者の電子署名32、電子鍵33、アクセス制御情報34もその対象となる。

【0025】次に、クライアントのエージェント起動者またはエージェント生成者は、エージェント1の持つデータ4またはエージェント1、セキュリティメカニズム2、セキュリティ情報3に対するアクセス制御情報34を生成する。

【0026】次に鍵管理メカニズム23は、データの暗号化に必要な電子鍵である共通鍵331を生成する。暗号・復号メカニズム22は、この共通鍵331を使ってデータに暗号化処理を施す。この時に暗号化処理の対象となるデータは、エージェント1とエージェント1の持つデータ4であるが、必要に応じてハッシュ値31、ア

4

クセス制御情報34もその対象となる。共通鍵331によって暗号処理が終わった後、暗号・復号メカニズム22は、その共通鍵331をサービス提供者の公開鍵332で暗号化処理したものが電子鍵33となる。

【0027】次に暗号・復号メカニズム22はエージェント起動者の秘密鍵333を使って、データに対してエージェント起動者の電子署名32を生成する。この時に対象となるデータは、エージェント1とエージェント1が持つデータ4であるが、必要に応じてハッシュメカニズム21、暗号・復号メカニズム22、鍵管理メカニズム23、アクセス制御メカニズム24、ハッシュ値31、電子鍵33、アクセス制御情報34もその対象となる。

【0028】全ての処理が終わった後、エージェント1はセキュリティメカニズム2とセキュリティ情報3と共にサーバマシンへ移動する。

【0029】次に図4、図5、図6を用いて本発明のサーバマシンでのセキュリティ処理方式を説明する。図4に示すように、サーバマシン側では、先に説明したハッシュメカニズム21、暗号・復号メカニズム22、鍵管理メカニズム23、アクセス制御メカニズム24、ハッシュ値31、エージェント起動者の電子署名32、電子鍵33、アクセス制御情報34とサービス提供プログラム10から構成される。また、サーバでは、事前に暗号・復号メカニズム22やサービス提供プログラム10の復号・電子署名識別処理に必要な、起動者の公開鍵335、サービス提供者の秘密鍵334を保持しておく必要がある。

【0030】サービス提供プログラム10は エージェント1から要求のあるサービスを提供する機能、 エージェント起動者の電子署名の識別機能、 暗号化されたデータの復号処理機能、 エージェントを強制終了させる機能を持つモジュールである。

【0031】図5、図6を使ってエージェントでのセキュリティ処理例を説明する。

【0032】初めに、サービス提供プログラム10はエージェント起動者の電子署名32を起動者の公開鍵335を使って識別する。サービス提供プログラム10は、この識別処理から誰が署名したかを確認し、その署名者からのエージェントを実行させて良いかどうかを判断する。必要ならエージェントを強制終了させる。

【0033】次に、鍵管理メカニズム23は電子鍵33をサービス提供プログラム10に渡す。サービス提供プログラム10は受け取った電子鍵33をサービス提供者の秘密鍵334で復号処理を行い、共通鍵331を入手し、鍵管理メカニズム23に渡す。鍵管理メカニズム23は、共通鍵331を暗号・復号メカニズム22に渡す。暗号・復号メカニズム22は、共通鍵331を使って暗号処理されているデータの復号を行う。データは、クライアントで暗号処理されたデータである。

10

20

30

40

50

【0034】ハッシュメカニズム21はデータに対するハッシュ値を計算し、転送されてきたハッシュ値31と比較する。データは、クライアントでハッシュ処理されたデータである。

【0035】サービス提供プログラム10が、エージェント1、データ4、ハッシュメカニズム21、暗号・復号メカニズム22、鍵管理メカニズム23、アクセス制御メカニズム24、ハッシュ値31、エージェント起動者の電子署名32、電子鍵33、アクセス制御情報34に対してアクセス要求してきた場合、アクセス制御メカニズム24はアクセス制御情報34を基にアクセスを制御する。

【0036】サーバマシン上にセキュリティメカニズム2でセキュリティ処理エラーが発生した場合、エージェント1は全ての処理を中断し、クライアントへ移動する。

【0037】

【発明の効果】以上説明したように、本発明によれば、エージェント自身に暗号処理を施すことができるので、第三者による機密の漏洩やエージェントの不正使用を防ぐという効果がある。また、セキュリティメカニズムやアルゴリズムはエージェント自身が持ち、一緒に移動することができるので、クライアント、サーバとも相手がサポートしているセキュリティメカニズム、アルゴリズムを気にしないで、セキュリティを保護することができるという効果もある。また、アクセス制御メカニズムを持つことができるので、エージェントやそれが持つセキュリティメカニズム、セキュリティ情報へのアクセスを制御することができるという効果もある。また、エージェントと共に電子署名を送付できるので、サーバマシン側で不要なエージェントの実行を制御できるという効果もある。また、本発明ではサービス提供プログラムは自分の秘密鍵をエージェント又はセキュリティメカニ

ムに渡さないシステムなので、秘密鍵の不正な複製、利用を防止できるという効果もある。さらに、本発明ではエージェントに対する電子署名はエージェント起動者のみとしているので、エージェントの起動者を識別することができるという効果もある。

【図面の簡単な説明】

【図1】本発明の一実施例に基づくエージェントセキュリティを示す図である。

【図2】クライアントマシンでのセキュリティ処理方式の一例を示す図である。

【図3】クライアントマシンでのセキュリティ処理の流れの一例を示す図である。

【図4】サーバマシンでのセキュリティ処理方式の一例を示す図である。

【図5】エージェントでのセキュリティ処理の流れの一例を示す図である。

【図6】サービス提供プログラムでのセキュリティ処理の流れの一例を示す図である。

【符号の説明】

- 10…サービス提供プログラム、
- 21…ハッシュメカニズム、
- 22…暗号・復号メカニズム、
- 23…鍵管理メカニズム、
- 24…アクセス制御メカニズム、
- 31…ハッシュ値、
- 32…エージェント起動者の電子署名、
- 33…電子鍵、
- 34…アクセス制御情報、
- 331…共通鍵、
- 332…サービス提供者の公開鍵、
- 333…起動者の秘密鍵、
- 334…サービス提供者の秘密鍵、
- 335…起動者の公開鍵。

【図1】

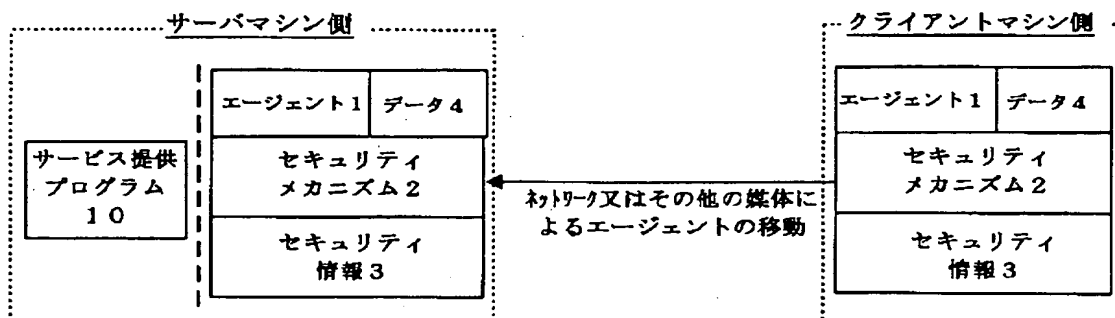


図1

【図2】

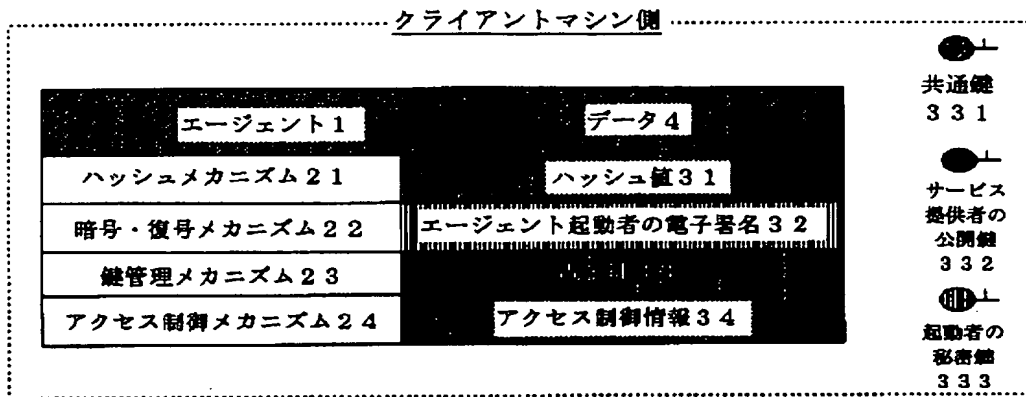


図2

【図3】

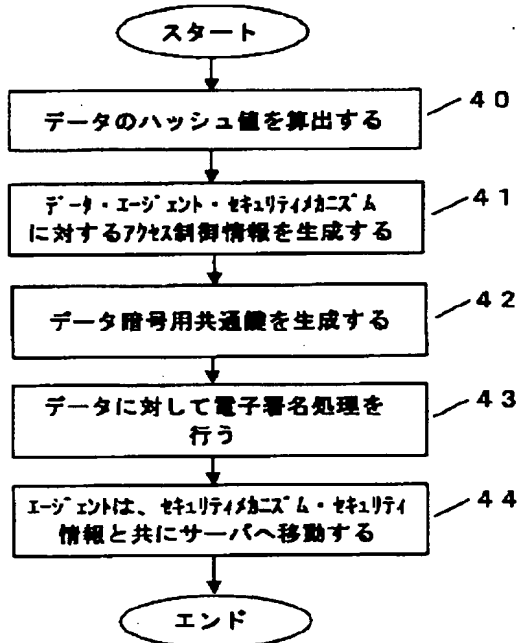


図3

【図5】

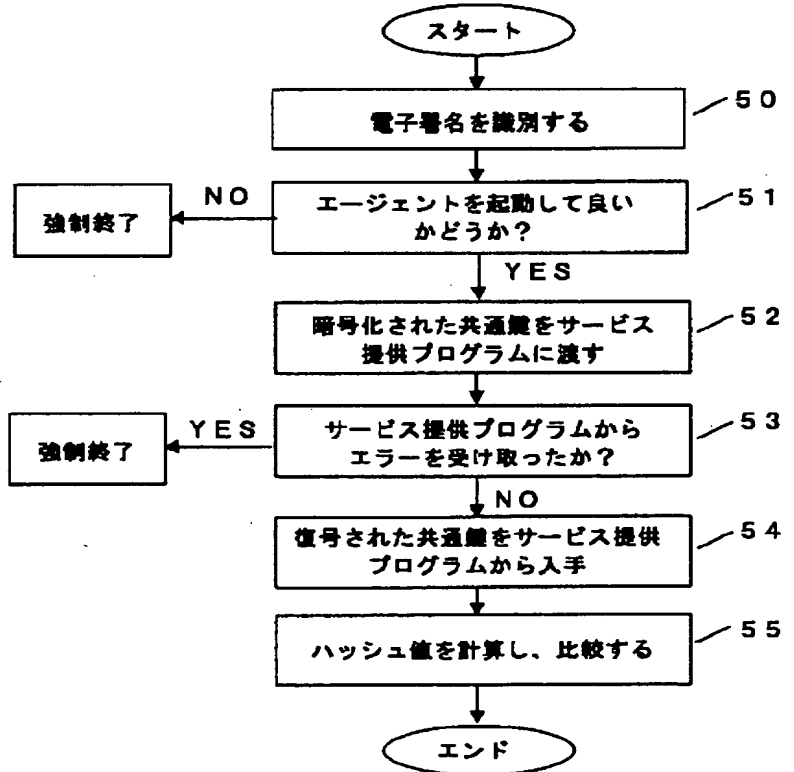


図5

【図4】

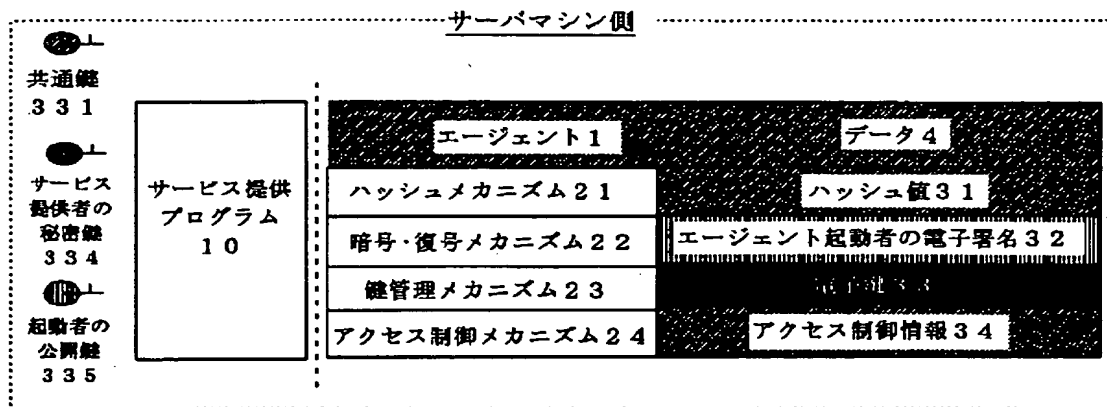


図4

【図6】

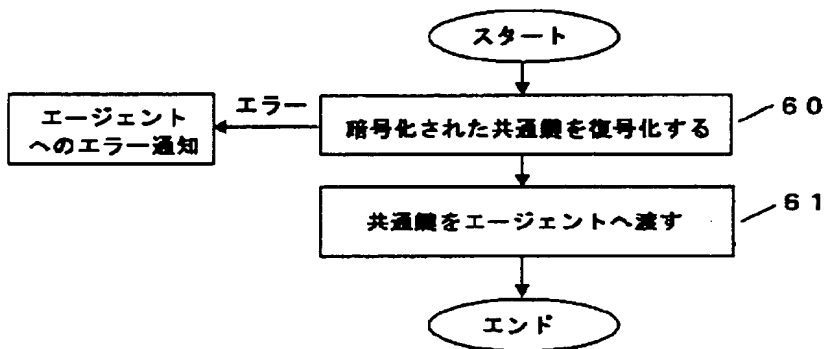


図6

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.